

# KEEPING UP WITH CHINA: CFIUS AND THE NEED TO SECURE MATERIAL NONPUBLIC TECHNICAL KNOWLEDGE OF AI/ML

ANTHONY SEVERIN<sup>†</sup>

## ABSTRACT

*Artificial intelligence (AI) and machine learning (ML) technologies will shape societies by the values they are programmed to respect. In part because of anti-competitive Chinese practices such as forced transfers of intellectual property (IP), companies based in the U.S. have lost the ability to compete in several fields. To avoid losing competitiveness in AI/ML sectors, the Committee on Foreign Investment in the United States (CFIUS) should promulgate rules blocking Chinese investors from acquiring ownership interests in U.S. companies when that ownership would allow access to material nonpublic technical knowledge of AI/ML. Such a categorical blacklist approach will limit forced transfers of IP and increase the influence of American values on the development of AI/ML technology.*

*“Until recently, the internet in almost every country outside China has been defined by American platforms with strong free expression values. There’s no guarantee these values will win out. A decade ago, almost all of the major internet platforms were American. Today, six of the top ten are Chinese.”*

*Mark Zuckerberg<sup>1</sup>*

## INTRODUCTION

In January 2020, the Department of the Interior announced that it had grounded its entire drone fleet.<sup>2</sup> Though these drones made more than 10,000 flights in 2018 to help monitor endangered species and survey

---

<sup>†</sup> Duke University School of Law, J.D. expected, May 2021; Baylor University, B.S., December 2014.

<sup>1</sup> *Mark Zuckerberg Stands for Voice and Free Expression*, FACEBOOK (Oct. 17, 2019), <https://about.fb.com/news/2019/10/mark-zuckerberg-stands-for-voice-and-free-expression/> (“We can continue to stand for free expression, understanding its messiness, but believing that the long journey towards greater progress requires confronting ideas that challenge us. Or we can decide the cost is simply too great. I’m here today because I believe we must continue to stand for free expression”).

<sup>2</sup> Lisa Friedman & David McCabe, *Interior Dept. Grounds Its Drones Over Chinese Spying Fears*, N.Y. TIMES (Jan. 30, 2019), <https://www.nytimes.com/2020/01/29/technology/interior-chinese-drones.html>.

federal land (among other uses),<sup>3</sup> the department grounded the fleet over concerns that the drones' Chinese manufacturers might have backdoors or data collection functions which enable cyber espionage.<sup>4</sup> The Department had purchased Chinese-manufactured drones mainly because they are recognized as the best in the industry: Chinese-owned companies control more than eighty percent of the market for small unmanned aerial vehicles.<sup>5</sup> Pentagon officials have since remarked on the need for U.S. manufacturers to regain parity with their Chinese counterparts to ensure a "safe and secure supply" of domestically manufactured drones.<sup>6</sup>

Drones are but one technology with a supply chain that has national security implications for all countries. Acknowledging this, China promulgated the Made in China 2025 ("MIC 2025") strategic initiative, aiming to secure market share in ten industries.<sup>7</sup> These industries include next-generation information technology, robotics, aerospace and aviation equipment, and new energy vehicles, among others.<sup>8</sup> The Chinese government subsidizes companies in these fields when they achieve certain goals such as localizing intellectual property (IP).<sup>9</sup>

China's goal of localizing IP has implications for the U.S. and its allies in part because of the way China uses foreign direct investment (FDI) to accomplish this goal.<sup>10</sup> The Chinese government frequently invests in foreign companies with substantial IP assets,<sup>11</sup> either directly or through a state-owned enterprise (SOE). This investment gives the government access to proprietary information and technical know-how, which it may then transfer to all Chinese companies. An example of a "forced IP transfer," this process gives a competitive advantage to Chinese producers relative to their U.S.-based counterparts because the profit motive that would drive protection of IP assets does not apply to SOEs. China has begun to use this ability to distort the market to its strategic advantage.

American responses to forced IP transfers have ramped up. In 2018, the U.S. Trade Representative (USTR) issued a two-tiered list of

---

<sup>3</sup> U.S. DEP'T OF THE INTERIOR, UNMANNED AIRCRAFT SYSTEMS (UAS) PROGRAM 2018 USE REP. 4 (2019).

<sup>4</sup> Friedman & McCabe, *supra* note 2.

<sup>5</sup> Lukas Schroth, *Drone Manufacturer Market Shares: DJI Leads the Way in the US*, DRONE INDUSTRY INSIGHTS (Sept. 26, 2019), <https://www.droneii.com/drone-manufacturer-market-shares-dji-leads-the-way-in-the-us>.

<sup>6</sup> Transcript, Ellen M. Lord, *Undersecretary of Defense Lord Holds Press Briefing on Acquisition Reform and Innovation* (Aug. 26, 2019), <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1944326/undersecretary-of-defense-lord-holds-press-briefing-on-acquisition-reform-and-i/>.

<sup>7</sup> WAYNE M. MORRISON, CONG. RESEARCH SERV., IF10964, THE MADE IN CHINA 2025 INITIATIVE: ECONOMIC IMPLICATIONS FOR THE UNITED STATES 2 (2019).

<sup>8</sup> U.S. Chamber of Commerce, MADE IN CHINA 2025: GLOBAL AMBITIONS BUILT ON LOCAL PROTECTIONS 10 (2017), [https://www.uschamber.com/sites/default/files/final\\_made\\_in\\_china\\_2025\\_report\\_full.pdf](https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf).

<sup>9</sup> *Id.* at 48.

<sup>10</sup> See MORRISON, *supra* note 7.

<sup>11</sup> *Id.*

products on which it would apply a twenty-five percent tariff.<sup>12</sup> The list targeted products benefitting from the above-described forced transfers of IP.<sup>13</sup> Additionally, Congress enacted the Foreign Investment Risk Review Modernization Act (FIRRMA), which gave more authority to the Committee on Foreign Investment in the United States (CFIUS) to block certain investments by foreign entities.

Building on these policy reactions, CFIUS should promulgate rules blocking Chinese investors from acquiring ownership interests in U.S. companies when that ownership would allow access to material nonpublic technical knowledge<sup>14</sup> in artificial intelligence (AI) and machine learning (ML). While this would limit the short-run availability of FDI, failing to address the issue of forced technology transfers may place the U.S. at a permanent technological disadvantage.

## I. BACKGROUND

### A. AI and National Security

Failing to maintain parity in ML technologies with other nations would be detrimental to U.S. national security. A simple scenario, feasible with existing technology,<sup>15</sup> illustrates why: an unidentified group creates several hundred “deepfakes”—that is, fake video and audio—which feature Presidential candidates from both political parties making disturbing statements. Social distrust would spread as voters debate whether the videos are real, potentially destabilizing the election cycle or increasing volatility in financial markets. A variety of other more direct military applications of ML technologies are possible, such as impersonating military leadership via natural language processing,<sup>16</sup> pattern recognition which speeds review of intelligence,<sup>17</sup> and use of ML-driven tools in cyber operations.<sup>18</sup> Further, commentators have widely noted the lack of a civilian-military distinction within the country.<sup>19</sup> Non-dual-use technology could become dual-use.

---

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> See 50 U.S.C. § 4565 (a)(4)(D)(i)(1).

<sup>15</sup> See John Feffer, *Will a ‘Deepfake’ Swing the 2020 Election?*, FOREIGN POL’Y FOCUS (Jun. 19, 2019), <https://ips-dc.org/deepfake-swing-2020-election/>.

<sup>16</sup> 2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM, *AI: Using Standards to Mitigate Risks* 12 (2018), [https://www.dni.gov/files/PE/Documents/2018\\_AEP-AI.pdf](https://www.dni.gov/files/PE/Documents/2018_AEP-AI.pdf).

<sup>17</sup> *Id.* at 13.

<sup>18</sup> See Greg Allen & Taniel Chan, *Artificial Intelligence and National Security* 18 (Jul. 2017), <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security> (quoting Adm. Mike Rogers, director of the National Security Agency, who suggests that “Artificial Intelligence and machine learning . . . is foundational to the future of cybersecurity”).

<sup>19</sup> Andrew P. Hunter et al., *Artificial Intelligence and National Security: The Importance of the AI Ecosystem*, CTR. FOR STRATEGIC AND INT’L STUD. 49 (2018), [https://csis-prod.s3.amazonaws.com/s3fspublic/publication/181102\\_AI\\_interior.pdf](https://csis-prod.s3.amazonaws.com/s3fspublic/publication/181102_AI_interior.pdf).

Maintaining AI/ML parity may result in solutions to these threats. Automated deepfake detection technology already exists,<sup>20</sup> with major companies releasing training datasets of deepfaked videos to help improve detection.<sup>21</sup> More importantly, technological parity would ensure that the technology is at least partially shaped by American interests in freedom of expression and privacy rather than by those with interests in maximizing surveillance and control.<sup>22</sup>

AI/ML parity is no guarantee, however, given China's centrally directed efforts and investments made in its pursuit of MIC 2025. China is actively investing in U.S.-based companies with "militarily relevant" ML technical knowledge.<sup>23</sup> From 2010-2017, Chinese-based investors ramped up investment in emerging technologies, participating in \$1.3 billion investments in the field over that time and accounting for 29 percent of Chinese FDI in 2017.<sup>24</sup> IP owned by U.S.-based companies with Chinese investors is at risk of being forcibly transferred. In 2017, the Chinese Cybersecurity Law became effective, requiring certain companies doing business in China to keep certain data on local Chinese-based servers<sup>25</sup> and allow certain government officials full access.<sup>26</sup> This law has raised concerns that firms could be asked to provide source code or other IP to the Chinese government,<sup>27</sup> which would allow the code to be illicitly shared with state-owned enterprises (SOEs).

### *B. AI/ML as Uniquely Critical Technologies*

It is becoming popular to suggest that AI is mostly a buzzword and is not a big deal.<sup>28</sup> Given the failure of other technological buzzwords

---

<sup>20</sup> David Guera & Edward J. Delp, *Deepfake Video Detection Using Recurrent Neural Networks*, Video and Image Processing Laboratory at Purdue University (2018), <https://engineering.purdue.edu/~dgueraco/content/deepfake.pdf>.

<sup>21</sup> Alex Engler, *Fighting Deepfakes When Detection Fails*, BROOKINGS INSTITUTION (Nov. 14, 2019), <https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/>.

<sup>22</sup> See KELLEY M. SAYLER, CONG. RESEARCH SERV., R45178, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 22 (2019) ("Some experts believe that China's intent to be the first to develop military AI applications may result in comparatively less safe applications as China will likely be more risk-acceptant throughout the development process.").

<sup>23</sup> *Id.* at 21.

<sup>24</sup> Michael Brown & Pavneet Singh, *China's Technology Transfer Strategy*, DEF. INNOVATION UNIT EXPERIMENTAL 7 (2018), [https://admin.govexec.com/media/diux\\_chinatechnologytransferstudy\\_jan\\_2018\\_\(1\).pdf](https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf).

<sup>25</sup> Wangluoanquan Fa Quan (网络安全法全) [Cyber Security Law] (promulgated by the Nat'l People's Cong, Nov. 7, 2016, effective Jun. 1, 2017), art. 37.

<sup>26</sup> Wangluoanquan Fa Quan (网络安全法全) [Cyber Security Law] (promulgated by the Nat'l People's Cong, Nov. 7, 2016, effective Jun. 1, 2017), art. 28.

<sup>27</sup> See Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, THE DIPLOMAT (Jun. 1, 2017), <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/> ("The law has raised concerns among some foreign companies over greater data controls as well as increased risks of intellectual property theft.").

<sup>28</sup> See, e.g., Eric Siegel, *Why A.I. is a Big Fat Lie*, BIGTHINK (Jan. 23, 2019), <https://bigthink.com/technology-innovation/why-a-i-is-a-big-fat-lie>.

to impress—like blockchain<sup>29</sup>—this makes some sense. AI provides ways of doing things better and more quickly, but it does not seem to fundamentally revolutionize the tasks to which it has been applied.

But AI will improve. It is not a bold prediction to say that in twenty years, AI *will* be able to fundamentally revolutionize more tasks, and it will shape those tasks in ways that imbue certain values. Surveillance cameras with built in ML-driven facial recognition technology, for example, seem creepy to some but normal to others. How society chooses to implement technology will define norms for future generations.

Moreover, AI is particularly prone to monopolies. AI is driven by data and data processing. Sorting data into a useful format is frequently difficult, at least for the moment. Moreover, even if we should conquer that problem, the primary barrier to improving AI algorithms is the time it takes to train a model on such a large amount of data. Especially when AI can experiment (such as with human users by showing them different recommendations and incorporating those reactions into the model),<sup>30</sup> organizations that have been around for longer and have more data will usually have the upper hand against market entrants. Thus, should China or the U.S. gain a strategic advantage against the other, it may prove difficult for one to dislodge the other.

## II. EXISTING LAW

CFIUS may suspend transactions, mergers, or joint ventures resulting in a foreign person having control over any U.S. business if the transaction would pose a risk to national security.<sup>31</sup> At CFIUS's recommendation, the President may then block the transaction permanently.<sup>32</sup> "Covered transactions" are generally outlined by statute, and include those resulting in a foreign person having access to "material nonpublic information,"<sup>33</sup> or have involvement in substantive decision-making of U.S. businesses regarding critical infrastructure<sup>34</sup> and critical technologies,<sup>35</sup> or control over a business which has certain sensitive personal data about U.S. citizens.<sup>36</sup> Transactions of certain real estate may also be covered.<sup>37</sup>

CFIUS may review transactions *sua sponte*<sup>38</sup> or because a party to the transaction formally notifies CFIUS in advance and seeks specific

---

<sup>29</sup> See, e.g., Ben Dickson, *Are We in a Blockchain Winter?*, PCMag (Apr. 6, 2019), <https://www.pcmag.com/commentary/367612/are-we-in-a-blockchain-winter>.

<sup>30</sup> See CGP Grey, *How Machines Learn*, YOUTUBE (Dec. 18, 2017), <https://www.youtube.com/watch?v=R9OHn5ZF4Uo>.

<sup>31</sup> 50 U.S.C. § 4565(l)(1).

<sup>32</sup> 50 U.S.C. § 4565(d)(1).

<sup>33</sup> 50 U.S.C. § 4565(a)(4)(D)(i)(I).

<sup>34</sup> 50 U.S.C. § 4565(a)(4)(D)(i)(III)(bb).

<sup>35</sup> 50 U.S.C. § 4565(a)(4)(D)(i)(III)(cc).

<sup>36</sup> 50 U.S.C. § 4565(a)(4)(D)(i)(III)(aa).

<sup>37</sup> 50 U.S.C. § 4565(a)(4)(C).

<sup>38</sup> 50 U.S.C. § 4565(b)(1)(D).

approval.<sup>39</sup> Once CFIUS approves a transaction for which approval was specifically sought, it may not be re-reviewed.<sup>40</sup>

The Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018 substantially expanded CFIUS's authority in important ways.<sup>41</sup> Major changes included allowing the Committee to treat investors from specified countries differently,<sup>42</sup> allowing it to promulgate rules requiring mandatory filing for certain transactions,<sup>43</sup> and broadening the scope of the Committee's purview to include certain real estate and personally identifiable data relating to U.S. citizens.<sup>44</sup> FIRRMA also provided for a \$20 million expansion of CFIUS's appropriation, presumably to handle its newly-delegated authority and prominence as a newfound centerpiece of national security law.<sup>45</sup>

### A. Legislative History

Established in 1975 pursuant to an Executive Order, President Ford created CFIUS to address concerns that certain investments by OPEC members were politically rather than economically motivated.<sup>46</sup> The Order focused on data collection and descriptive analysis and did not provide the power to impede foreign investment.<sup>47</sup>

In response to concerns that the President lacked authority to collect this sort of data absent legislative mandate, Congress passed the International Investment Survey Act of 1976 to give the President the “‘clear and unambiguous authority’ to collect information on ‘international investment.’”<sup>48</sup>

It was not until the 1988 “Exon-Florio” amendment to the Defense Production Act that Congress delegated to the President the authority to block certain acquisitions of U.S. businesses.<sup>49</sup> The President could only exercise that authority, however, if “(1) other U.S. laws were inadequate or inappropriate to protect the national security and (2) ‘credible evidence’ existed that the foreign interest exercising control might take action that threatened to impair U.S. national security.”<sup>50</sup>

The most dramatic change in CFIUS's statutory authority came with the passage of the Foreign Investment and National Security Act of 2007 (FINSA), which, among other changes, drastically broadened the number of transactions covered by adding to the list of factors which

---

<sup>39</sup> 50 U.S.C. § 4565(b)(1)(C).

<sup>40</sup> 31 C.F.R. § 800.601 (2019).

<sup>41</sup> See JAMES K. JACKSON, CONG. RESEARCH SERV., R33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 2 (Feb. 14, 2020).

<sup>42</sup> 50 U.S.C. § 4565(a)(4)(E).

<sup>43</sup> John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115–232 § 1706, 132 Stat. 1636, 2184 (2018).

<sup>44</sup> 50 U.S.C. § 4565(a)(4)(C).

<sup>45</sup> See JACKSON, *supra* note 41, at 12.

<sup>46</sup> *Id.* at 4.

<sup>47</sup> *Id.* at 5–6.

<sup>48</sup> *Id.* at 6.

<sup>49</sup> *Id.* at 7.

<sup>50</sup> *Id.*

CFIUS could use to determine if a transaction impaired national security.<sup>51</sup> New factors added by the 2007 law included effects on “critical infrastructure” or “critical technologies,” as well as “such other factors as the President or the Committee determine to be appropriate.”<sup>52</sup> FINSA also created measures intended to boost transparency and reporting to Congress.<sup>53</sup>

Congress enacted the Export Control Reform Act of 2018 (ECRA) along with FIRRMA. The ECRA places export controls on products which are identified as “foundational and emerging technologies” and “essential to the national security of the United States.”<sup>54</sup> Acquisitions of businesses with products subject to controls under this provision of the ECRA are then incorporated by reference as “critical technologies” subject to CFIUS review.<sup>55</sup> While existing export control provisions cover software like encryption tools,<sup>56</sup> there is no general limitation on the export of AI/ML algorithms.

### *B. Final Rules*

In September 2019, Treasury proposed permanent rules to replace the pilot program.<sup>57</sup> These rules became effective in February 2020.

Most relevant to this note’s proposal is the rules’ creation of an investor whitelist. FIRRMA required the Committee to define what a “foreign person” means and to “limit the application of such clauses to the investments of certain categories of foreign persons.”<sup>58</sup> When the rules were initially proposed, they did not specify exempted countries.<sup>59</sup> Rather, they left the list to a vote of CFIUS members.<sup>60</sup>

The House Financial Services Committee criticized this decision. In their October 2019 letter, the House Committee’s leadership wrote to express their desire that “many U.S. allies, including NATO and non-NATO partners, should remain unaffected by FIRRMA’s expansion,” and

---

<sup>51</sup> JACKSON, *supra* note 41, at 10.

<sup>52</sup> 50 U.S.C. § 4565(f)(11). If this seems overbroad to the point of making the other factors redundant, that’s because it is overbroad. To borrow a phrase from a commentator, “[t]he Committee’s legal mandate is replete with discretion.” David Zaring, *CFIUS as Congressional Notification Service*, 83 S. CAL. L. REV. 81, 84 (2009). FINSA’s broadening of the scope of transactions covered by CFIUS is a possible legislative reaction to CFIUS’s failure to intervene in a purchase of six U.S. ports by Dubai Ports World in 2006. See JACKSON, *supra* note 41, at 4.

<sup>53</sup> See JACKSON, *supra* note 41, at 10.

<sup>54</sup> 50 U.S.C. § 4817(a).

<sup>55</sup> 50 U.S.C. § 4565(a)(6)(A)(vi).

<sup>56</sup> 15 C.F.R. § 742.15.

<sup>57</sup> Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. 50,174 (Sep. 24, 2019) [hereinafter Notice] (to be codified at 31 C.F.R. pt. 800).

<sup>58</sup> 50 U.S.C. § 4565(a)(4)(E).

<sup>59</sup> Notice, *supra* note 57, at 50,179.

<sup>60</sup> *Id.*

urged the Committee to establish a list as soon as possible.<sup>61</sup> In response, the Committee has “initially selected” Australia, Canada, and the United Kingdom as excepted foreign states,<sup>62</sup> implying that more additions may be made.

Comments submitted on the proposed rules argued that the mandatory filing requirements were onerous and made investors more hesitant<sup>63</sup> and businesses more inclined to exclude foreign investors when possible.<sup>64</sup> The comments argued that this burden would be particularly heavy in fields like biotechnology and venture capital, where deals and technology move very quickly.<sup>65</sup>

Direct impacts on Chinese FDI are already becoming clear. Chinese venture investment declined in the U.S. during the first half of 2019, about 27 percent over the preceding two quarters.<sup>66</sup> However, some commentators have noted that “CFIUS appears ill-equipped to police the venture-capital industry,”<sup>67</sup> raising questions about compliance rates in industries related to AI and ML technologies.

There is a clear desire among stakeholders for categorical rules and regulatory certainty. Of all the submissions during the public comment period,<sup>68</sup> by far the most common request was for the Committee to act quickly to add their preferred country to the whitelist.<sup>69</sup> Others did not explicitly request a country to be added to the whitelist, but rather requested published criteria so they could understand what guidelines

---

<sup>61</sup> H. COMM. ON FIN. SERVICES, HOUSE LETTER TO SECRETARY MNUCHIN ON FIRRM DRAFT RULES 2 (Oct. 17, 2019), <https://www.regulations.gov/document?D=TREAS-DO-2019-0008-0065>.

<sup>62</sup> Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3,112, 3,116 (Jan. 17, 2020) (to be codified at 31 C.F.R. pt. 800).

<sup>63</sup> See, e.g., SHEARMAN & STERLING, Comment on Proposed Rule NPRM Part 800 – Provisions Pertaining to Certain Investments in the United States by Foreign Persons 2 (Oct. 17, 2019), <http://www.regulations.gov/document?D=TREAS-DO-2019-0008-0054> (noting the proposed rule creates “a strong incentive for Japanese companies to exclude non-Japanese nationals from a non-excepted foreign state in order to avoid a mandatory CFIUS filing”).

<sup>64</sup> *Id.*

<sup>65</sup> See Genentech, Inc., Comments on the Proposed Provisions Pertaining to Certain Investments in the United States by Foreign Persons 3 (Oct. 16, 2019), <https://www.regulations.gov/document?D=TREAS-DO-2019-0008-0051>.

<sup>66</sup> Heather Somerville, *China Investors Keep Making Deals in Silicon Valley Amid Washington Pushback*, WALL ST. J. (Oct. 28, 2019), <https://www.wsj.com/articles/chinese-investors-u-s-tech-entrepreneurs-continue-to-make-deals-11572275105>.

<sup>67</sup> *Id.*

<sup>68</sup> Your author has read all of them. The volume of well-drafted and almost certainly well-compensated comments makes clear the need for disinterested commentary on the subject.

<sup>69</sup> See, e.g., SHEARMAN & STERLING, *supra* note 63.



needed to be met to be on the whitelist.<sup>70</sup> This reflects a larger desire for transparency which partly motivates this paper's proposal.

### *C. Ralls and Other Limitations on Authority of CFIUS*

Some commentators note that the law covers “potentially tens of thousands [of transactions] each year.”<sup>71</sup> But “[w]hile CFIUS's reach is broad, it is not infinite.”<sup>72</sup> What limitations exist?

The constitution provides some constraint, explored for the first and only time by a court in *Ralls Corporation v. Committee on Foreign Investment in the United States*.<sup>73</sup> Ralls was a U.S.-based company owned by two Chinese nationals. In 2012, Ralls purchased four companies with assets allowing development of wind farms in Oregon within restricted airspace and near a bombing zone maintained by the U.S. Navy.<sup>74</sup> Ralls then notified the Committee of the acquisition and responded to several questions but was never informed of the significance of CFIUS's inquiries.<sup>75</sup> In the following months, the Committee ordered Ralls to suspend the wind farm's development and conducted an investigation.<sup>76</sup> After the investigation and finding that Ralls “might take action that threatens to impair the national security of the United States,” the President issued a divestment order which required Ralls to sell its interest in the wind farms.<sup>77</sup>

Ralls contended that, under the Due Process Clause,<sup>78</sup> it was entitled to know the grounds on which CFIUS made its decision and be given the opportunity to present its side to the Committee. A three-judge panel of the D.C. Circuit agreed: its 2014 opinion held that “due process requires, at the least, that an affected party be informed of the official action, be given access to the unclassified evidence on which the official actor relied and be afforded an opportunity to rebut that evidence.”<sup>79</sup>

*Ralls* has come under fire from multiple sides. Some argue that it requires the executive to surrender information that should properly be

---

<sup>70</sup> See, e.g., Nancy McLernon, *Comments on Provisions Pertaining to Certain Investments in the United States by Foreign Persons*, 84 Fed. Reg. 50,174 and *Provisions Pertaining to Certain Transactions by Foreign Persons Involving Real Estate in the United States*, 84 FR 50214, ORG. FOR INT'L INVESTMENT 2 (Oct. 17, 2019), <https://www.regulations.gov/document?D=TREAS-DO-2019-0008-0048>.

<sup>71</sup> Farhad Jalinous et al., *CFIUS Reform Becomes Law: What FIRRMA Means for Industry*, WHITE & CASE 2 (2018), <https://www.whitecase.com/sites/whitecase/files/files/download/publications/cfius-reform-becomes-law-what-firma-means-for-industry.pdf>.

<sup>72</sup> *U.S. Export Controls and the Committee on Foreign Investment in the United States (CFIUS) Before the H. Comm. on Foreign Affairs*, 115th Cong. 2 (2018) (statement of Hon. Marco Mancuso, Senior Visiting Fellow, Hudson Institute).

<sup>73</sup> 758 F.3d 296 (D.C. Cir. 2014).

<sup>74</sup> *Id.* at 304.

<sup>75</sup> *Id.* at 305.

<sup>76</sup> *Id.*

<sup>77</sup> *Id.* at 306.

<sup>78</sup> *Ralls Corp.* 758 F.3d, at 306.

<sup>79</sup> *Id.* at 319.

subject to executive privilege and part of the executive's inherent authority to maintain international relations.<sup>80</sup> Other commentators suggest that *Ralls* does not do enough to protect property interests.<sup>81</sup>

The other major limitation on CFIUS's authority over covered transactions is its own rules. As one commentator remarks, "[t]he negotiated solution [to CFIUS's expansive authority] appears to be deferring to CFIUS to 'prescribe regulations' . . . ."<sup>82</sup>

### III. CREATING CATEGORICAL RULES PROHIBITING CERTAIN INVESTMENT

#### A. Proposal

CFIUS should adopt rules that block Chinese investors from acquiring ownership interests in U.S. companies if that ownership would allow access to material nonpublic technical knowledge in AI/ML. This approach is a categorical blacklist, as opposed to the individualized, *ad hoc* assessments in current practice.

#### B. Statutory Authorization for the Proposal

CFIUS has statutory authority to implement a categorical prohibition like the one proposed. FIRRMA explicitly authorizes the Committee to single out an individual country for greater scrutiny,<sup>83</sup> such as China in this proposal. In fact, in commenting on the existing proposed rules, a letter from the House Committee on Financial Services noted that "Treasury has opted for a so-called white list interpretation instead of a black list [sic]," but that "such an approach is not compulsory under FIRRMA."<sup>84</sup> Rather, the law merely requires Treasury to define what a "foreign person" means and to "limit the application of such clauses to the investments of certain categories of foreign persons,"<sup>85</sup> which it has chosen to do through an as-yet-to-be-promulgated whitelist. This paper argues in favor of a blacklist approach.

#### C. Categorical Rules and *Ralls*

A categorical rule like the one offered here could be subject to challenge on the grounds that *Ralls* procedural due process<sup>86</sup> requires an individualized assessment of each blocked transaction.

---

<sup>80</sup> See Christopher M. Fitzpatrick, *Where Ralls Went Wrong: CFIUS, the Courts, and the Balance of Liberty and Security*, 101 CORNELL L. REV. 1087, 1111 (2016).

<sup>81</sup> See Yang Wang, *Incorporating the Third Branch of Government Into U.S. National Security Review of Foreign Investment*, 38 HOUS. J. INT'L L., 323, 345 (2016).

<sup>82</sup> Jalinous, *supra* note 71, at 2.

<sup>83</sup> See 50 U.S.C. § 4565(a)(4)(E). The proposed rules currently under consideration do not use this authority to target any particular country. See CATHLEEN D. CIMINO-ISAACS & JAMES K. JACKSON, CONG. RESEARCH SERV., IF11334, CFIUS: NEW FOREIGN INVESTMENT REVIEW REGULATIONS 2 (2019).

<sup>84</sup> H. COMM. ON FIN. SERVICES, *supra* note 61.

<sup>85</sup> 50 U.S.C. § 4565(a)(4)(E).

<sup>86</sup> *Ralls* is the controlling precedent as challenges to CFIUS actions must be brought in the D.C. Circuit. See 50 U.S.C. § 4565(e)(2).

Certain factors not present in *Ralls* would act in the government's favor in a new case, however. The *Ralls* Court mentioned,<sup>87</sup> and it has been widely noted in the literature,<sup>88</sup> that the government in that case simply did not raise the issue of executive privilege until oral arguments at the appellate level.<sup>89</sup> This oversight may have left a persuasive argument unexplored. Additionally, the enactment of FIRRMA four years after *Ralls* decidedly reaffirmed Congress' intent to delegate substantial power to the Committee. Given the broad language of FIRRMA, it is difficult to imagine what actions might be beyond the power Congress intended to delegate.

A strong analogy exists between the discretion given to CFIUS to identify national security risks and the President's authority under the International Emergency Economic Powers Act (IEEPA) to declare emergencies. In the leading case on the subject, *Dames & Moore v. Regan*, the Court was unbothered by the infringement on economic liberty by the President's powers under IEEPA.<sup>90</sup>

The *Ralls* court was able to distinguish *Dames & Moore* by noting that the transaction in *Ralls* had already been completed, and thus the property right had been fully vested.<sup>91</sup> But a categorical rule like this proposal would bar future transactions, where property rights had not yet been vested. The critical distinction drawn by the *Ralls* Court would not be possible in a future review of this paper's proposal.

#### D. Discussion

China has consolidated control of the majority of market share in many sectors, including drones,<sup>92</sup> telecom equipment,<sup>93</sup> surveillance cameras,<sup>94</sup> and internet-of-things devices.<sup>95</sup> These categories of devices have serious privacy and data security concerns.<sup>96</sup> The Department of

---

<sup>87</sup> *Ralls Corp.*, 758 F.3d at 320–21.

<sup>88</sup> See Fitzpatrick, *supra* note 80, at 1109 (noting that “the precedent that the President set by releasing such a vast amount of information is problematic because it represents a surrender to the judiciary’s interference in the CFIUS process”).

<sup>89</sup> *Ralls Corp.*, 758 F.3d at 319.

<sup>90</sup> See *Dames & Moore v. Regan*, 453 U.S. 654 (1981).

<sup>91</sup> See *Ralls Corp.*, 758 F.3d at 316 (noting that “*Ralls*’s state-law property rights fully vested upon the completion of the transaction, meaning due process protections necessarily attached”).

<sup>92</sup> Schroth, *supra* note 5.

<sup>93</sup> John Chen et al., *China’s Internet of Things*, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION 1 (2008), [https://www.uscc.gov/sites/default/files/Research/SOSi\\_China's%20Internet%20of%20Things.pdf](https://www.uscc.gov/sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf).

<sup>94</sup> Paul Mozur et al., *Made in China, Exported to the World: The Surveillance State*, N.Y. TIMES (Apr. 24, 2019), <https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html>.

<sup>95</sup> Chen, *supra* note 93.

<sup>96</sup> See *id.* at 128 (noting that “[t]he Chinese government has given itself nearly unchecked legal powers to harness the data and supply chains of Chinese civilian firms for uses ranging from espionage to offensive operations” which “creates the potential for an unresolved critical tension between the commercial interests of

Defense is spending millions to reignite domestic innovation and manufacturing in these sectors, and these technologies are relatively straightforward to manufacture and design. Conversely, AI/ML technologies are particularly vulnerable to runaway leaders. Many AI/ML solutions interact with huge quantities of data and improve as they are used.<sup>97</sup> This creates a kind of network effect that entrenches the front runner. If China pulls ahead, the U.S. may never catch up.<sup>98</sup>

### 1. Economic Impacts.

The benefits of FDI are well established and vital to the continued growth of the U.S. economy.<sup>99</sup> Failing to “consistently attract sufficient (benign) FDI into the U.S. would present a long-term, systemic national security risk.”<sup>100</sup> Beyond the macro effects, however, are the micro effects on individual businesses. Blocking all non-passive FDI in ML technology will almost certainly reduce short-run innovation. Some commentators have suggested that this might send technical expertise away from Silicon Valley and to China.<sup>101</sup>

The premise of this note is, however, is that FDI is *already* driving the U.S. inexorably towards that end. FDI will merely ensure a future monopoly over high-end ML technology via forced technology transfers. That monopoly would have a chilling effect on innovation, as cheaper and better foreign products flood the U.S. market but with no way for U.S. companies to build on these products. This note’s proposal for a categorical rule would engender the creation and maintenance of a self-sustaining cycle of innovation instead of allowing IP to be slowly siphoned away.

Moreover, Chinese FDI accounts for a relatively limited portion of total investment stock. In 2017, FDI into the United States exceeded \$4

---

Chinese firms wishing to sell IoT products in the United States and the security and privacy of U.S. citizens”).

<sup>97</sup> See Matt Turck, *The Power of Data Network Effects*, MATTTURCK.COM (Jan. 4, 2016), <https://mattturck.com/the-power-of-data-network-effects/> (noting that “the more users use your product, the more data they contribute; the more data they contribute, the smarter your product becomes”).

<sup>98</sup> China already enjoys a substantial lead in data collection and availability due to lax privacy protections. See Natalie Sherman, *Is China gaining an edge in artificial intelligence?*, BBC (Nov. 12, 2019), <https://www.bbc.com/news/business-50255191> (“If the government decides that it’s going to have country-wide electronic medical records . . . then it’s going to happen.” (quoting Tom Mitchell)).

<sup>99</sup> See John K. Mullen & Martin Williams, *Foreign Direct Investment and Regional Economic Performance*, 58 KYKLOS 265, 279 (2005) (“We find that inward foreign investment plays a strong, vital role in regional economic activity.”).

<sup>100</sup> Mancuso, *supra* note 72.

<sup>101</sup> See Justin Shields, Note, *Smart Machines and Smarter Policy: Foreign Investment Regulation, National Security, and Technology Transfer in the Age of Artificial Intelligence*, 51 J. MARSHALL L. REV. 279, 298 (2018) (“U.S. regulatory action also has the potential to deprive the U.S. AI industry of knowledge inputs from Chinese firms and Chinese talent that can increase the competitiveness of the industry.”).

trillion.<sup>102</sup> Of that amount, 84 percent was by European, Canadian, and Japanese investors,<sup>103</sup> traditional allies which would likely be considered excepted countries under the Committee's whitelist.

As tensions have risen between the U.S. and China in recent years, commentators have begun to fear the "The Great Decoupling."<sup>104</sup> Decoupling refers to the bifurcation of economies, social structures, and technological development in a way reminiscent of the Cold War.

The decoupling has already begun; indeed, China and the U.S. have never been fully coupled. The Great Firewall, for example, has made American tech giants largely powerless to achieve the market dominance that they have seen elsewhere in the world.<sup>105</sup> Social media networks, usually driven by network effects,<sup>106</sup> are likewise powerless as China has walled itself off to promote its domestic alternatives.<sup>107</sup>

While the transitional period away from reliance on Chinese FDI may cause market headwinds, the U.S. should be able to mitigate the effects of decoupling and avoid isolating itself. It must reinvest in its allies. It could do so through a "multilateral regime under which firms subject to potential government influence in their corporate decision-making must demonstrate their 'eligibility' to engage in outbound M&A."<sup>108</sup> This could take the form of categorical rules providing for a whitelist, as in the Committee's proposed rules.

---

<sup>102</sup> DANIEL J. IKENSON, *ECONOMIC BEDROCK: HOW INTERNATIONAL COMPANIES BOOST AMERICA'S ECONOMIC ADVANTAGE 2* (2018), [http://ofii-docs.ofii.org/dmfile/Economic-Bedrock-Report\\_Final.pdf](http://ofii-docs.ofii.org/dmfile/Economic-Bedrock-Report_Final.pdf).

<sup>103</sup> *Id.*

<sup>104</sup> Mario Mancuso et al., *3 Policy Developments to Watch as US-China Divide Grows*, *LAW360* (Oct. 9, 2019), <https://www.law360.com/articles/1208004/3-policy-developments-to-watch-as-us-china-divide-grows>.

<sup>105</sup> See Robin Wauters, *China Blocks Access To Twitter, Facebook After Riots*, *TECHCRUNCH* (Jul. 7, 2009), <https://techcrunch.com/2009/07/07/china-blocks-access-to-twitter-facebook-after-riots/> (noting that both Facebook and Twitter were blocked after riots in 2009).

<sup>106</sup> See Bertand Belvaux, *The Development of Social Media: Proposal for a Diffusion Model Incorporating Network Externalities in a Competitive Environment*, 26 *RECHERCHE ET APPLICATIONS EN MARKETING*, 7, 17 (2011) ("Consequently, if it has a large market share, the social medium grows more through the network externalities mechanism. If, on the other hand, it has a small market share, it attracts few new adopters.").

<sup>107</sup> There is nothing particularly unique about China's ability to create its own social network aside from the Great Firewall, which has left Chinese citizens with no other readily available choices. Other countries such as Egypt and Russia have shown their willingness to limit access to social media. Your author expects similar, localized and country specific social media networks to rise in the coming years, leading to inevitable segmentation. In many ways, the current dominance of western social media platforms in other countries is an anomaly which will likely soon be challenged by the rise of nationalism.

<sup>108</sup> Jeffrey Gordon & Curtis Milhaupt, *China as a "National Strategic Buyer": Towards a Multilateral Regime for Cross-Border M&A*, 2019 *COLUM. BUS. L. REV.* 192, 193 (2019).

## 2. Transparency

Commentators have noted that “relatively little is known about CFIUS decision-making and the types of evidence that are used.”<sup>109</sup> Much to the chagrin of the burgeoning crop of national security lawyers in large firms thriving on this uncertainty,<sup>110</sup> a bright-line standard prohibiting all transactions of this type would turn an expansive and expensive regulation into a yes-or-no question for all but certain edge cases. This standard would reduce transaction costs dramatically and enable investors to make acquisitions more quickly, without having to wait for CFIUS approval or enduring the uncertainty of not requesting a review.

A categorical approach like the one proposed here would also improve CFIUS’s credibility. CFIUS currently appears arbitrary: a survey of Chinese investors in 2016 found that 43 percent thought the CFIUS process was “politically charged.”<sup>111</sup> Another 43 percent expressed lack of knowledge; only 13 percent expressed a positive view.<sup>112</sup>

In 2010, CFIUS voted not to block a Russian acquisition of a uranium mining company, Uranium One.<sup>113</sup> It was later revealed that the Clinton Foundation had received various donations from a several involved parties.<sup>114</sup> As it turns out, then-Secretary of State Hillary Clinton was only tangentially involved, and the vote, which involved representatives from many agencies, was unanimous.<sup>115</sup> But those facts have not stopped the issue from being a recurring theme in national discourse years after the events.<sup>116</sup> Categorical rules like the one proposed in this paper would provide regulatory certainty and limit the ground for Uranium One-style controversy.

## 3. Ethical Development of AI/ML Technology.

Some commentators have suggested that closing off the market would be tantamount to ceding U.S. authority.<sup>117</sup> On the contrary, recent

<sup>109</sup> Wang, *supra* note 81.

<sup>110</sup> See David Zaring, *Administration by Treasury*, 95 MINN. L. REV. 187, 198–99 (2010) (noting that “it is an administrative regime rarely studied by scholars or reviewed by courts, but one that is very lawyered up. Lawyers representing clients before [CFIUS] . . . comprise one of the fastest growing bars in Washington D.C. and New York City, with at least five lawyers from antitakeover specialists Wachtell Lipton recently authoring papers on how to navigate the process.”).

<sup>111</sup> Ji Li, *I Came, I Saw, I... Adapted: An Empirical Study of Chinese Business Expansion in the United States and its Legal and Policy Implications*, 36 NW. J. INT’L L. & BUS. 143, 178 (2016).

<sup>112</sup> *Id.*

<sup>113</sup> E. Maddy Berg, *A Tale of Two Statutes: Using IEEPA’s Accountability Safeguards to Inspire CFIUS Reform*, 118 COLUM. L. REV. 1763, 1763–64.

<sup>114</sup> *Id.*

<sup>115</sup> See Paul Rosenzweig, *Unpacking Uranium One: Hype and Law*, LAWFARE (Oct. 27, 2017), <https://www.lawfareblog.com/unpacking-uranium-one-hype-and-law> (noting that “[i]t is unlikely that Secretary Clinton personally participated in the transaction”).

<sup>116</sup> *Id.*

<sup>117</sup> See Shields, *supra* note 101, at 298.

experience shows that robust market demand will keep tech companies interested enough to change practices. The General Data Privacy Regulation (GDPR)—which ostensibly applies only within the EU—has forced changes by every major tech company worldwide.<sup>118</sup> Instead of forcing a flight of tech companies from Europe, it has imposed quintessentially European perspectives on data privacy on monolithic tech firms.<sup>119</sup> Limiting investment may create a similar greenhouse in the U.S. where it can exercise ethical leadership. As a Pentagon official noted in a recent press conference:

It's become circular — if you want to make sure that there are ethics principles that are attached to AI, you have to have the AI . . . . [I]f other people have the AI and you don't, then you're already in second place and you can't really do anything about making sure there are ethical principles involved.<sup>120</sup>

### CONCLUSION

AI/ML technologies will shape societies by the values they are programmed to respect. In part because of Chinese anti-competitive practices, the United States has lost the ability to compete in several fields, including commercial drones,<sup>121</sup> surveillance cameras,<sup>122</sup> and some telecom equipment.<sup>123</sup> It would be disastrous if the U.S. lost parity with AI/ML technologies in the same way.

CFIUS, as powerful as it has become, has intervened in only a handful of transactions<sup>124</sup> despite its portrayal by detractors as “shadowy.”<sup>125</sup> It has been cautious with its power. But when a clear threat arises, and Congress has delegated power to deal with that threat, a president and her officers must act. China is spending millions of dollars to secure American IP, and those investments drain long-term staying power from the U.S. economy in exchange for short term influxes of cash.

---

<sup>118</sup> Julian Vigo, *How Tech Culture Has Changed Since The GDPR*, FORBES (May 5, 2019), <https://www.forbes.com/sites/julianvigo/2019/05/05/how-tech-culture-has-changed-since-the-gdpr/>.

<sup>119</sup> *Id.*

<sup>120</sup> Daniel Wilson, *New Ethics Framework May Draw AI Firms To DOD*, LAW360 (Nov. 8, 2019), <https://www.law360.com/articles/1217965/new-ethics-framework-may-draw-ai-firms-to-dod>.

<sup>121</sup> See Schroth, *supra* note 5.

<sup>122</sup> See Chen, *supra* note 93.

<sup>123</sup> See Mozur, *supra* note 94.

<sup>124</sup> See JAMES K. JACKSON & CATHLEEN D. CIMINO-ISAACS, CONG. RESEARCH SERV., IF10952, CFIUS REFORM: FOREIGN INVESTMENT NATIONAL SECURITY REVIEWS 2 (Oct. 3, 2019) (noting that prior to FIRRMA, the President has used CFIUS to block only five transactions).

<sup>125</sup> See Eric Platt, Opinion, *Shadowy US Security Committee Opens New Front with Grindr Sale*, FIN. TIMES (Mar. 29, 2019), <https://www.ft.com/content/1b9ab2b0-51c8-11e9-b401-8d9ef1626294> (characterizing CFIUS as “shadowy”).

The president of the Massachusetts Institute of Technology, L. Rafael Reif, penned an editorial in the New York Times discussing the relative technological advantages of the U.S. and China.<sup>126</sup> He writes:

If all we do in response to China's ambition is to try to double-lock all our doors, I believe we will lock ourselves into mediocrity. But if we in the United States respect China as a rising competitor with many strengths we can learn from, that view will inspire America to be its incomparable best.<sup>127</sup>

Reif is right. The strength of the U.S. and its tech sector is not within the borders of the U.S. alone, but is in its position as a superpower leading liberal democracies across the globe. This paper's proposal is not alone a solution. Rather, CFIUS should be one piece of a larger strategy.

But it is a necessary piece. To preserve American competitiveness and ethical leadership<sup>128</sup> in the next generation of technological advancement, CFIUS should take decisive and categorical action to defend American enterprise and abandon the piecemeal and cautious approach it has thus far employed.

---

<sup>126</sup> L. Rafael Reif, Opinion, *China's Challenge Is America's Opportunity*, N.Y. TIMES (Aug. 8, 2018), <https://www.nytimes.com/2018/08/08/opinion/china-technology-trade-united-states.html>.

<sup>127</sup> *Id.*

<sup>128</sup> See Ben Thompson, *The Internet and the Third Estate*, STRATECHERY (Oct. 21, 2019), <https://stratechery.com/2019/the-internet-and-the-third-estate> (“To fight the Internet’s impact, instead of seeking to understand it and guide the fundamental transformations that will surely follow, is a commitment by the West to lose the fight for the future.”).